Listing of Claims

Claims 1-27 (canceled)

Claim 28 (omitted in error due to improper numbering)

Claims 29-34 (canceled)

Claim 35 (amended) A method for verifying the security of an electronic transaction between a vendor providing a purchased item or service and a purchaser from that vendor to authenticate the transaction amount and the identity of the vendor, said method comprising the steps of:

the purchaser obtaining from the vendor transaction information identifying the transaction including the purchase amount ;

at the purchaser, electronically performing a message authentication code function on the transaction information and purchaser identification information including a secret key of the purchaser's to obtain secure information regarding the transaction and the purchaser;

providing the purchaser identification information and the secure information to the vendor;

the vendor transmitting the vendor transaction information, the purchaser identification information, and the secure information to a verifier;

the verifier using the purchaser's secret key to perform the same message authentication code function on the purchaser identification and the transaction information received from the vendor to determine whether the result of the verifier message authentication code function is the same as the secure information provided to the verifier by the vendor; and

if the result is the same, verifying the security of the electronic transaction.

Claim 36 (canceled)

Claim 37 (amended) The method of claim ~~36~~ 35 wherein the secure information is obtained by the step of performing a message authentication code function on at least some of the transaction information and purchaser information including a secret key of the purchaser's and the secure information is provided to the vendor as at least a part of a credit card number.

Claim 38 (amended) The method of claim 35 further comprising the step of adding a counter value to the ~~transition~~ transaction information prior to electronically performing the message authentication code function at the purchaser so that multiple purchases of the same item, from the same vendor, on the same day may be separately validated.

39. (amended) An apparatus for verifying the security of an electronic transaction between a vendor providing a purchased item or service and a purchaser of that vendor, said apparatus comprising:

~~a first~~ an input at the ~~user~~ purchaser for receiving from the vendor transaction information identifying the transaction including the purchase amount;

a ~~first~~ processor at the purchaser configured to receive the transaction information, purchaser identification information, and a purchaser secret key and electronically to perform a message authentication code function on the transaction information and the purchaser identification information using the secret key to obtain secure information regarding the transaction and the user;

~~a first~~ an output at the purchaser configured to output the result of the message authentication code function to the vendor;

a verifier;

~~a first~~ an input at a the verifier for receiving from the vendor the vendor transaction information, the purchaser identification information, and the secure information;

a ~~second~~ processor at the verifier for using the purchaser's secret key to perform the same message authentication code function on the purchaser identification information and the transaction information received from the ~~vender~~ vendor to determine whether the result of the verifier message authentication code function is the same as the secure information provided to the verifier by the vendor; and

~~a second~~ an output at the verifier for outputting a verification of the security of the electronic transaction if the result of the verifier message authentication code function is identical to the received secure information.

Claim 40 (canceled)

Claim 41 (amended) The apparatus of claim ~~39~~ 38 wherein said secure information includes at least a part of a credit card number.